

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-53668

(43) 公開日 平成11年(1999) 2月26日

(51) Int.Cl. ⁶	識別記号	F I	
G 0 8 B 25/04		G 0 8 B 25/04	K
G 0 6 F 12/14	3 2 0	G 0 6 F 12/14	3 2 0 B
17/30		H 0 4 M 11/04	
H 0 4 L 12/437		G 0 6 F 15/40	3 1 0 F
12/02		H 0 4 L 11/00	3 3 1
審査請求 未請求 請求項の数 6 O L (全 14 頁) 最終頁に続く			

(21) 出願番号 特願平9-206177

(22) 出願日 平成9年(1997) 7月31日

(71) 出願人 000237156

株式会社エフ・エフ・シー
東京都日野市富士町1番地

(72) 発明者 西田 廣治

東京都日野市富士町1番地 富士ファコム
制御株式会社内

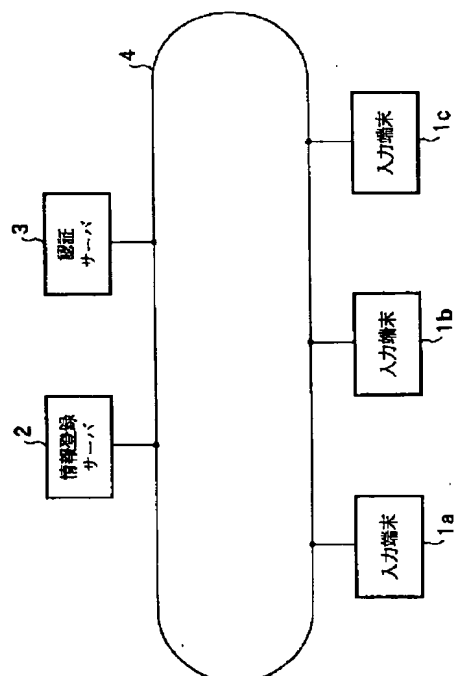
(74) 代理人 弁理士 森 哲也 (外3名)

(54) 【発明の名称】 災害時情報システム

(57) 【要約】

【課題】 災害発生の際に、救助活動や復旧活動を適切かつ早急に行うために必要な個人情報を好適に提供することのできる災害時情報システムを提供する。

【解決手段】 個人に関する個人情報として、少なくとも医療に必要な身体情報および住所または居所に関する所在情報を入力して暗号化する入力端末と、入力端末で暗号化された個人情報を登録する個人情報登録装置と、を接続し、災害発生の際に、個人情報登録装置に登録されている個人情報を特定者に復号化して提供する。



【特許請求の範囲】

【請求項 1】 個人に関する個人情報として、医療行為に必要な身体情報及び住所又は居所に関する所在情報を少なくとも入力して暗号化する入力端末と、前記入力端末で暗号化された前記個人情報を登録する個人情報登録装置と、を接続し、災害発生の際に、前記個人情報登録装置に登録されている前記個人情報を特定者に復号化して提供することを特徴とする災害時情報システム。

【請求項 2】 個人に関する個人情報として、医療行為に必要な身体情報及び住所又は居所に関する所在情報を少なくとも入力するための入力端末と、前記入力端末で入力された前記個人情報を登録する個人情報登録装置と、をネットワークに接続し、

前記入力端末は、入力された前記個人情報を特定の暗号キーで暗号化する暗号化処理と、前記暗号化処理により暗号化された前記個人情報を前記個人情報登録装置に送信する送信処理と、を実行し、且つ、前記個人情報を利用する適格を有する特定者の要求に応じて前記個人情報登録装置から前記個人情報を取得する取得処理と、前記取得処理により取得された前記個人情報を前記特定の暗号キーに対応する特定の復号キーで復号化する復号化処理と、を実行し、

前記個人情報登録装置は、前記入力端末から送信された前記個人情報を登録する登録処理と、災害発生の際に前記入力端末からの要求に応じて前記登録処理により登録された前記個人情報を前記入力端末に提供する提供処理と、を実行することを特徴とする災害時情報システム。

【請求項 3】 前記個人情報を送信しようとする先が前記個人情報登録装置であるか否かを認証するための第 1 の認証装置を前記ネットワークに接続し、前記入力端末は、前記第 1 の認証装置を利用し、前記個人情報を送信しようとする先が前記個人情報登録装置であると認証したときに、前記送信処理を実行することを特徴とする請求項 2 記載の災害時情報システム。

【請求項 4】 前記個人情報には、前記個人の安否に関する安否情報が含まれていることを特徴とする請求項 1、2 又は 3 記載の災害時情報システム。

【請求項 5】 前記個人と特定の関係を有する関係者の公開鍵を登録した第 2 の認証装置を前記ネットワークに接続し、

前記入力端末は、前記取得処理を実行する際に、前記関係者から入力された前記公開鍵に対応する秘密鍵で暗号化した認証情報を前記個人情報登録装置に送信し、前記個人情報登録装置から前記個人情報を取得したときに、前記個人情報を前記秘密鍵で復号化し、

前記個人情報登録装置は、前記入力端末から前記認証情報が送信された場合に、前記第 2 の認証装置から前記関係者の前記公開鍵を取得し、取得した前記公開鍵で前記認証情報を復号化し、前記認証情報が正常に復号化されたときに、前記個人情報を前記公開鍵で暗号化して前記

入力端末に提供することを特徴とする請求項 2、3 又は 4 記載の災害時情報システム。

【請求項 6】 前記関係者の金銭の額を管理する金額管理装置を前記ネットワークに接続し、前記入力端末は、災害発生の際に、前記関係者の要求に応じて前記金額管理装置で管理されている前記関係者の金銭の額を義援金として提供することを特徴とする請求項 5 記載の災害時情報システム。

【発明の詳細な説明】**【0001】**

【発明の属する技術の分野】本発明は、災害発生の際に、あらかじめ登録した個人情報を、その利用適格を有する特定者に提供する災害時情報システムに関する。

【0002】

【従来の技術】従来、個人に関する情報として、病院のカルテに記載される医療情報や自己所有の金銭の額に関する金額情報、住所または居所の建物の間取り図や緊急連絡先などは、その多くが紙面や狭域内に設けられたデータベースなどに記録され、それぞれ独立に管理されていた。

【0003】

【発明が解決しようとする課題】ところで、従来、災害発生の際には、これら個人情報を利用することにより、医療活動に従事する医師や救護活動に従事する救護員または消防要員などが適切に救助活動を行えたり、本人またはその家族等が早急に復旧活動を行えたりすることが望まれていた。

【0004】しかしながら、病院のカルテに記載される医療情報や自己所有の金銭の額に関する金額情報などの個人情報は、病院内や銀行間でのみ利用が限定されたデータベースにより管理されており、しかも、個人情報を利用する権限を有する者でなければ、例えば家族等であっても利用することができない場合があった。

【0005】また、情報が統括して管理されていないため、医療活動に従事する医師や救護活動に従事する救急要員または消防要員、本人や家族等は、必要な情報ごとに、その情報があるところまで赴かなければ、これを得ることができなかった。

【0006】そこで、本発明は、このような従来の問題を解決することを課題としており、災害発生の際に、救助活動や復旧活動を適切かつ早急に行うために必要な個人情報を好適に提供することのできる災害時情報システムを提供することを目的としている。

【0007】

【課題を解決するための手段】上記目的を達成するために、本発明に係る請求項 1 記載の災害時情報システムは、個人に関する個人情報として、医療行為に必要な身体情報および住所または居所に関する所在情報を少なくとも入力して暗号化する入力端末と、前記入力端末で暗号化された前記個人情報を登録する個人情報登録装置

と、を接続し、災害発生の際に、前記個人情報登録装置に登録されている前記個人情報を特定者に復号化して提供する。

【0008】このような構成であれば、災害が発生していない通常のときには、本人、家族等、医師、公営機関または建築業者などが入力端末を利用し、医療情報や所在情報などの個人情報を入力する。そうすると、入力端末では、入力された個人情報が暗号化されて個人情報登録装置に送信される。個人情報登録装置では、入力端末から送信された個人情報が登録される。

【0009】一方、災害が発生したときには、個人情報を利用する適格を有する特定者が入力端末を利用し、個人情報の提供を要求する。そうすると、入力端末では、特定者からの要求に応じて、個人情報登録装置に対して個人情報の提供が要求される。個人情報登録装置では、個人情報の提供を要求している者が特定者であると確認されたときに、登録されている個人情報が入力端末に提供される。そして、このとき、提供される個人情報は、入力端末または個人情報登録装置で復号化されて特定者に提供される。

【0010】なお、災害が発生していない通常のときに限らず、いかなるときであっても、個人情報を入力端末に入力して個人情報登録装置に登録するようにしてもよいし、災害が発生していない通常のときにのみ、個人情報を入力端末に入力して個人情報登録装置に登録するようにしてもよい。

【0011】この請求項1記載の発明において、身体情報とは、医療行為に必要な情報であって、例えば、病院のカルテに記載される情報である。また、所在情報とは、住所または居所に関する情報であって、例えば、住所若しくは居所そのもの、住所若しくは居所に係る電話番号、住所若しくは居所に係る建物の間取り図、住所若しくは居所を含む周辺の地図、または緊急連絡先である。さらに、特定者とは、個人情報を利用する適格を有する者であって、例えば、本人若しくは家族等、または、災害発生の際に、医療活動に従事する医師、救護活動に従事する救護員、国若しくは救助活動を指揮する地方自治体の責任者である。

【0012】また、本発明に係る請求項2記載の災害時情報システムは、個人に関する個人情報として、医療行為に必要な身体情報および住所または居所に関する所在情報を少なくとも入力するための入力端末と、前記入力端末で入力された前記個人情報を登録する個人情報登録装置と、をネットワークに接続し、前記入力端末は、入力された前記個人情報を特定の暗号キーで暗号化する暗号化処理と、前記暗号化処理により暗号化された前記個人情報を前記個人情報登録装置に送信する送信処理と、を実行し、かつ、前記個人情報を利用する適格を有する特定者の要求に応じて前記個人情報登録装置から前記個人情報を取得する取得処理と、前記取得処理により取得

された前記個人情報を前記特定の暗号キーに対応する特定の復号キーで復号化する復号化処理と、を実行し、前記個人情報登録装置は、前記入力端末から送信された前記個人情報を登録する登録処理と、災害発生の際に前記入力端末からの要求に応じて前記登録処理により登録された前記個人情報を前記入力端末に提供する提供処理と、を実行する。

【0013】このような構成であれば、災害が発生していない通常のときには、本人、家族等、医師、公営機関または建築業者などが入力端末を利用し、医療情報や所在情報などの個人情報を入力する。そうすると、入力端末では、暗号化処理により、入力された個人情報が特定の暗号キーで暗号化され、送信処理により、暗号化された個人情報が個人情報登録装置に送信される。個人情報登録装置では、登録処理により、入力端末から送信された個人情報が登録される。

【0014】一方、災害が発生したときには、個人情報を利用する適格を有する特定者が入力端末を利用し、個人情報の提供を要求する。そうすると、入力端末では、特定者からの要求に応じて、取得処理により、個人情報登録装置に対して個人情報の提供が要求される。個人情報登録装置では、個人情報の提供を要求している者が特定者であると確認されたときに、提供処理により、登録されている個人情報が入力端末に提供される。そして、入力端末では、取得処理により、個人情報登録装置から個人情報が取得され、復号化処理により、取得された個人情報が特定の復号キーで復号化される。これにより、個人情報が特定者に提供される。

【0015】この請求項2記載の発明において、暗号キーとは、データを暗号化しようとするアルゴリズムを決定するための動機付けとなるものである。また、暗号キーと対応する復号キーとは、暗号化されているデータを復号化しようとするアルゴリズムを決定するための動機付けとなるものであって、暗号キーとデータを正常に復元するために必要な所定の因果関係を有するものである。これらには、データを暗号化するとき、または、暗号化データを復号化するときを設定するパスワードや、パスワードを要しない暗号化または復号化アルゴリズムであれば、そのアルゴリズムそのものを含むものである。

【0016】したがって、この請求項2記載の発明において、復号化とは、暗号化データの暗号キーと上記所定の因果関係を有している復号キーに基づいて、暗号化データを元のデータに正常に復元することであって、その暗号キーと上記所定の因果関係を有していない復号キーに基づいて、元のデータ以外のものを生成することは含まないものである。

【0017】さらに、本発明に係る請求項3記載の災害時情報システムは、請求項2記載の災害時情報システムにおいて、前記個人情報を送信しようとする先が前記個

個人情報登録装置であるか否かを認証するための第 1 の認証装置を前記ネットワークに接続し、前記入力端末は、前記第 1 の認証装置を利用し、前記個人情報を送信しようとする先が前記個人情報登録装置であると認証したときに、前記送信処理を実行する。

【0018】このような構成であれば、入力端末では、入力された個人情報が暗号化されると、第 1 の認証装置が利用され、個人情報を送信しようとする先が個人情報登録装置であるか否かが認証される。そして、送信しようとする先が個人情報登録装置であると認証されたときに、送信処理により、暗号化した個人情報が個人情報登録装置に送信される。

【0019】この場合において、個人情報登録装置を認証するには、例えば、第 1 の認証装置にあらかじめ正当な個人情報登録装置であることを示すための公開鍵を登録しておき、個人情報登録装置が登録してある公開鍵に対応する秘密鍵で認証情報を暗号化して入力端末に送信する。入力端末では、個人情報登録装置から認証情報を受信したときに、第 1 の認証装置から登録してある個人情報登録装置の公開鍵を取得し、その公開鍵で送信された認証情報を復号化し、正常に復号化することができるか否かを判定するようにすればよい。

【0020】個人に関する個人情報は、プライバシーに係わる情報であるため、厳重にその機密を保護しなければならない。入力端末と個人情報登録装置とが専用回線で接続されているような場合には特に問題はないが、インターネットなど複数のコンピュータが接続されているようなネットワークにこれらを接続するような場合には、入力端末が誤って異なるコンピュータに個人情報を送信してしまうおそれがある。そこで、上記のように、入力端末で、送信しようとする先が個人情報登録装置であるか否かを認証してから個人情報を送信するようにすれば、個人情報が漏洩する可能性を低減することができる。

【0021】さらに、本発明に係る請求項 4 記載の災害時情報システムは、請求項 1、2 または 3 記載の災害時情報システムにおいて、前記個人情報には、前記個人の安否に関する安否情報が含まれている。

【0022】さらに、本発明に係る請求項 5 記載の災害時情報システムは、請求項 2、3 または 4 記載の災害時情報システムにおいて、前記個人と特定の関係を有する関係者の公開鍵を登録した第 2 の認証装置を前記ネットワークに接続し、前記入力端末は、前記取得処理を実行する際に、前記関係者から入力された前記公開鍵に対応する秘密鍵で暗号化した認証情報を前記個人情報登録装置に送信し、前記個人情報登録装置から前記個人情報を取得したときに、前記個人情報を前記秘密鍵で復号化し、前記個人情報登録装置は、前記入力端末から前記認証情報が送信された場合に、前記第 2 の認証装置から前記関係者の前記公開鍵を取得し、取得した前記公開鍵で

前記認証情報を復号化し、前記認証情報が正常に復号化されたときに、前記個人情報を前記公開鍵で暗号化して前記入力端末に提供する。

【0023】このような構成であれば、個人と特定の関係を有する家族等の関係者が個人情報を取得しようとするには、関係者が入力端末を利用し、個人情報の提供を要求する。そうすると、入力端末では、関係者から入力された秘密鍵で認証情報が暗号化され、暗号化された認証情報が個人情報登録装置に送信される。個人情報登録装置では、個人情報の提供を要求した者の公開鍵が第 2 の認証装置から取得され、送信された認証情報が取得された公開鍵で復号化される。このとき、認証情報が正常に復号化されると、個人情報の提供を要求した者が個人情報を利用する適格を有する関係者であるものと判定され、該当する個人情報が公開鍵で暗号化され、入力端末に提供される。入力端末では、認証情報を暗号化したときと同一の秘密鍵で提供された個人情報が復号化される。これにより、個人情報が関係者に提供される。

【0024】さらに、本発明に係る請求項 6 記載の災害時情報システムは、請求項 5 記載の災害時情報システムにおいて、前記関係者の金銭の額を管理する金額管理装置を前記ネットワークに接続し、前記入力端末は、災害発生の際に、前記関係者の要求に応じて前記金額管理装置で管理されている前記関係者の金銭の額を義援金として提供する。

【0025】このような構成であれば、災害が発生したときに、関係者が被災地に義援金を提供しようとするには、関係者が入力端末を利用し、義援金を提供することを要求する。そうすると、入力端末では、関係者からの要求に応じて、金額管理装置に対して義援金の支払いが要求される。金額管理装置では、義援金の支払いが要求されると、支払いを要求した関係者が所有する金銭の額が義援金として提供される。

【0026】従来、義援金を提供しようとする者は、銀行や郵便局などを利用して義援金を被災地に提供していた。しかし、銀行や郵便局などに赴くために労力を要したり、またそこでの手続きが必要であったりすることなどが義援金を提供しようとする者を億劫にさせてしまい、積極的な義援活動が行われているとは言いがたかった。そこで、このように入力端末を利用することにより、簡単に義援金を提供できるようにすれば、多大な義援金の提供が期待され、支援活動が有効に行われることが期待される。

【0027】この請求項 5 記載の発明において、金額管理装置で管理される金銭の額とは、例えば、銀行の口座等で管理されるキャッシュ情報やクレジット情報である。

【0028】

【発明の実施の形態】以下、本発明の第 1 の実施の形態を図面を参照しながら説明する。図 1 は、本発明に係る

災害時情報システムによる第 1 の実施の形態を示すブロック図である。

【0029】この第 1 の実施の形態は、本発明に係る災害時情報システムを、図 1 に示すように、各地に設置された入力端末と、情報登録サーバと、認証サーバと、をネットワークに接続し、各入力端末で個人に関する個人情報を入力するとともに、災害発生の際に、登録されている個人情報を利用するのに適用したものである。

【0030】図中、個人情報を入力し且つ災害発生の際に個人情報を利用するための入力端末 1 a ~ 1 c と、入力端末 1 a ~ 1 c で入力された個人情報を登録し且つ災害発生の際に登録した個人情報を入力端末 1 a ~ 1 c に提供する情報登録サーバ 2 と、入力端末 1 a ~ 1 c および情報登録サーバ 2 間で送受信されるデータを認証するための認証サーバ 3 とは、データを伝送するためのデータ伝送路 4 で相互に接続されている。

【0031】入力端末 1 a ~ 1 c、情報登録サーバ 2 および認証サーバ 3 は、図 2 に示すように、同一機能を有して構成されており、演算およびシステム全体を制御する演算処理装置 5 と、データの読み出しおよび書き込みが可能な主記憶装置 6 および補助記憶装置 7 と、外部からのデータ入力可能なヒューマンインターフェースとしてのキーボード 8 と、キーボード 8 および外部とのデータの入出力を行うインターフェース部 9 と、主記憶装置 6 の特定領域に格納されているデータを画像信号に変換して出力する CRT 制御装置 10 と、CRT 制御装置 10 から出力された画像信号を画面に表示する CRT 11 と、で構成されており、演算処理装置 5、主記憶装置 6、補助記憶装置 7 およびインターフェース部 9 は、データを伝送するための信号線であるバスで相互に接続されている。

【0032】主記憶装置 6 は、あらかじめ演算処理装置 5 の制御プログラム等が格納されている ROM と、補助記憶装置 7 から読み込んだデータおよび演算処理装置 5 の演算過程に必要な演算結果を格納する RAM と、CRT 11 に表示するための表示データを蓄積する VRAM と、で構成されている。なお、VRAM は、演算処理装置 5 と CRT 制御装置 10 とで独立に、かつ、相互にアクセスが可能となっている。

【0033】補助記憶装置 7 は、FDD または HDD 等の不揮発性記憶媒体からなっている。そして、情報登録サーバ 2 の補助記憶装置 7 には、図 3 に示すように、入力端末 1 a ~ 1 c から送信される個人情報が格納されるようになっている。この場合に、個人情報は、個人情報に係る者の名前と、医療に必要な身体情報と、住所および居所やその電話番号などの連絡先情報と、住所および居所に係る建物の間取り図などの建物構造情報と、からなっている。また、認証サーバ 3 の補助記憶装置 7 には、図 4 に示すように、情報登録サーバ 2 に登録されている個人情報に係る者の名前と、その公開鍵と、が格納

されるようになっている。

【0034】CRT 制御装置 10 は、主記憶装置 6 の VRAM に格納されているデータを先頭アドレスから所定周期で順次読み出し、読み出したデータを画像信号に変換して CRT 11 に出力するように構成されている。

【0035】入力端末 1 a ~ 1 c の演算処理装置 5 は、マイクロプロセッシングユニット MPU 等からなり、個人情報を入力しようとするときには、主記憶装置 6 の ROM の所定領域に格納されている所定のプログラムを起動させ、図 5 (a) のフローチャートに示す処理を実行し、災害発生の際に、情報登録サーバ 2 に登録されている個人情報を利用しようとするときには、図 5 (b) のフローチャートに示す処理を実行するようになっている。

【0036】つまり、入力端末 1 a ~ 1 c の演算処理装置 5 で、個人情報を入力しようとするときに実行される処理は、次のように構成されている。まず、図 5 (a) に示すように、ステップ S 1 に移行して、個人情報をキーボード 8 より入力し、ステップ S 2 に移行して、入力した個人情報に係る者の公開鍵をキーボード 8 より入力し、ステップ S 3 に移行して、入力した個人情報に係る者の公開鍵で個人情報を暗号化し、ステップ S 4 に移行するようになっている。

【0037】ステップ S 4 では、情報登録サーバ 2 より認証情報を取得し、ステップ S 5 に移行して、認証サーバ 3 より情報登録サーバ 2 の公開鍵を取得し、ステップ S 6 に移行して、取得した情報登録サーバ 2 の公開鍵で認証情報を復号化し、ステップ S 7 に移行するようになっている。なお、ステップ S 4 で、情報登録サーバ 2 より取得する認証情報は、情報登録サーバ 2 の秘密鍵で暗号化されている。

【0038】ステップ S 7 では、認証情報が正常に復号化されたか否かを判定し、正常に復号化されたとき判定されたときには、ステップ S 8 に移行して、そうでないと判定されたときには、ステップ S 4 に移行するようになっている。ここで、取得される認証情報は、あらかじめ設定した所定の書式に基づいて作成されたものであり、正常に復号化されたか否かを判定するには、復号化した結果、所定の書式が検出されるか否かによって行うようになっている。

【0039】ステップ S 8 では、暗号化した個人情報を情報登録サーバ 2 に送信し、一連の処理を終了するようになっている。また、入力端末 1 a ~ 1 c の演算処理装置 5 で、災害発生の際に、情報登録サーバ 2 に登録されている個人情報を利用しようとするときに実行される処理は、次のように構成されている。まず、図 5 (b) に示すように、ステップ S 11 に移行して、要求する個人情報に係る者の名前をキーボード 8 より入力し、ステップ S 12 に移行して、要求する個人情報に係る者の秘密鍵をキーボード 8 より入力し、ステップ S 13 に移行し

て、要求する個人情報に係る者の秘密鍵で認証情報を暗号化し、ステップS 1 4に移行するようになっている。

【0040】ステップS 1 4では、暗号化した認証情報を情報登録サーバ2に送信し、ステップS 1 5に移行して、情報登録サーバ2より個人情報を受信したか否かを判定し、受信したと判定されたときには、ステップS 1 6に移行して、要求する個人情報に係る者の秘密鍵で受信した個人情報を復号化し、ステップS 1 7に移行して、復号化した個人情報をCRT 1 1に表示し、一連の処理を終了するようになっている。

【0041】一方、ステップS 1 5で、情報登録サーバ2より個人情報を受信しないと判定されたときには、ステップS 1 8に移行して、所定のエラー処理を実行し、一連の処理を終了するようになっている。

【0042】また一方、情報登録サーバ2の演算処理装置5は、マイクロプロセッシングユニットMPU等からなり、入力端末1 a ~ 1 cより個人情報の登録が要求されたときには、主記憶装置6のROMの所定領域に格納されている所定のプログラムを起動させ、図6 (a)のフローチャートに示す処理を実行し、災害発生の際に、入力端末1 a ~ 1 cより個人情報の提供が要求されたときには、図6 (b)のフローチャートに示す処理を実行するようになっている。

【0043】つまり、情報登録サーバ2の演算処理装置5で、入力端末1 a ~ 1 cより個人情報の登録が要求されたときに実行される処理は、次のように構成されている。まず、図6 (a)に示すように、ステップS 2 1に移行して、情報登録サーバ2の秘密鍵で認証情報を暗号化し、ステップS 2 2に移行して、暗号化した認証情報を登録要求のあった入力端末1 a ~ 1 cに送信し、ステップS 2 3に移行するようになっている。

【0044】ステップS 2 3では、登録要求のあった入力端末1 a ~ 1 cより個人情報を受信したか否かを判定し、受信したと判定されたときには、ステップS 2 4に移行して、受信した個人情報を補助記憶装置7の所定領域に登録し、一連の処理を終了するようになっている。

【0045】一方、ステップS 2 3で、登録要求のあった入力端末1 a ~ 1 cより個人情報を受信しないと判定されたときには、ステップS 2 5に移行して、所定のエラー処理を実行し、一連の処理を終了するようになっている。

【0046】また、情報登録サーバ2の演算処理装置5で、災害発生の際に、入力端末1 a ~ 1 cより個人情報の提供が要求されたときに実行される処理は、次のように構成されている。まず、図6 (b)に示すように、ステップS 3 1に移行して、入力端末1 a ~ 1 cより送信される認証情報を受信し、ステップS 3 2に移行して、要求のあった個人情報に係る者の公開鍵を認証サーバ3より取得し、ステップS 3 3に移行するようになっている。

【0047】ステップS 3 3では、要求のあった個人情報に係る者の公開鍵で認証情報を復号化し、ステップS 3 4に移行して、認証情報が正常に復号化されたか否かを判定し、正常に復号化されたと判定されたときには、ステップS 3 5に移行して、該当する個人情報を要求のあった入力端末1 a ~ 1 cに送信し、一連の処理を終了するようになっている。

【0048】一方、ステップS 3 4で、認証情報が正常に復号化されないと判定されたときには、ステップS 3 6に移行して、所定のエラー処理を実行し、一連の処理を終了するようになっている。

【0049】また一方、認証サーバ3の演算処理装置5は、マイクロプロセッシングユニットMPU等からなり、入力端末1 a ~ 1 cおよび情報登録サーバ2より公開鍵の提供要求がされたときには、主記憶装置6のROMの所定領域に格納されている所定のプログラムを起動させ、要求のあった個人情報に係る者の名前に該当する公開鍵を補助記憶装置7から読み込み、要求のあった入力端末1 a ~ 1 cまたは情報登録サーバ2に送信するようになっている。

【0050】次に、上記第1の実施の形態の動作を図面を参照しながら説明する。始めに、災害が発生していない通常のときに、本人、家族等、医師、公営機関または建築業者などがいずれかの入力端末1 a ~ 1 cを利用し、個人情報を情報登録サーバ2に登録する場合について説明する。

【0051】まず、本人、家族等、医師、公営機関または建築業者などが個人情報を情報登録サーバ2に登録しようとするには、各地に設置されているいずれかの入力端末1 a ~ 1 c、例えば入力端末1 aを利用し、個人情報に係る者の名前、身体情報、連絡先情報または建物構造情報などの個人情報を入力するとともに、個人情報に係る者の公開鍵を入力する。

【0052】そうすると、入力端末1 aでは、入力された個人情報が暗号化され、ステップS 4からS 7までを経て、個人情報を送信しようとする先が情報登録サーバ2であるか否かが認証され、送信しようとする先が情報登録サーバ2であると認証されたときに、暗号化された個人情報が情報登録サーバ2に送信される。

【0053】情報登録サーバ2では、入力端末1 aより個人情報が送信されると、補助記憶装置7にその個人情報が登録される。このとき、暗号化された個人情報は、図3に示すように、名前、身体情報、連絡先情報および建物構造情報のフィールドに区分され、個人情報ごとに1レコードとして登録される。

【0054】なお、入力端末1 aでは、個人情報を送信しようとする先が情報登録サーバ2でないと認証されたときには、情報登録サーバ2であると認証されるまで、ネットワークに接続されたコンピュータに対して認証を実行し続ける。また、情報登録サーバ2では、入力端末

1 a より個人情報の登録要求があったにもかかわらず、入力端末 1 a より個人情報が送信されないときには、エラー処理が実行される。

【0055】その次に、災害が発生した際に、本人若しくは家族等、または、医療活動に従事する医師、救護活動に従事する救護員、国若しくは救助活動を指揮する地方自治体の責任者などの個人情報を利用する適格を有する者（以下、特定者と称する）が、情報登録サーバ 2 に登録されている個人情報を救助活動等のために利用しようとする場合について説明する。

【0056】まず、特定者が情報登録サーバ 2 に登録されている個人情報を利用するには、各地に設置されているいずれかの入力端末 1 a ~ 1 c、例えば入力端末 1 b を利用し、利用しようとする個人情報に係る者の名前を入力するとともに、利用しようとする個人情報に係る者の秘密鍵を入力する。

【0057】そうすると、入力端末 1 b では、情報登録サーバ 2 に個人情報の提供が要求されるとともに、ステップ S 1 3、S 1 4 を経て、入力された秘密鍵に基づいて、情報登録サーバ 2 に対して個人情報を利用しようとする者が特定者であることが証明される。

【0058】情報登録サーバ 2 では、ステップ S 3 1 から S 3 4 までを経て、個人情報を利用しようとする者が特定者であると認証されると、該当する個人情報が入力端末 1 b に送信される。

【0059】入力端末 1 b では、情報登録サーバ 2 より個人情報が送信されると、個人情報に係る者の秘密鍵でその個人情報が復号化され、CRT 制御装置 1 0 により CRT 1 1 に表示される。

【0060】なお、情報登録サーバ 2 では、個人情報を利用しようとする者が特定者でないと認証されたときには、その旨が入力端末 1 b に送信される。入力端末 1 b では、これを受信すると、エラー処理が実行される。

【0061】このようにして、個人情報を入力して暗号化する入力端末 1 a ~ 1 c と、入力端末 1 a ~ 1 c で暗号化された個人情報を登録する情報登録サーバ 2 と、を接続し、災害発生の際に、情報登録サーバ 2 に登録されている個人情報を特定者に復号化して提供するようにしたから、救助活動や復旧活動を適切かつ早急に行うために必要な個人情報を好適に提供することができ、しかも、個人情報が漏洩する可能性を低減することができる。

【0062】特に、入力端末 1 a ~ 1 c では、入力された個人情報をその個人情報に係る者の公開鍵で暗号化し、暗号化した個人情報を情報登録サーバ 2 に送信するようにし、かつ、特定者の要求に応じて情報登録サーバ 2 から個人情報を取得し、取得した個人情報をその個人情報に係る者の秘密鍵で復号化するようにし、情報登録サーバ 2 では、入力端末 1 a ~ 1 c から送信された個人

らの要求に応じて登録されている個人情報を入力端末 1 a ~ 1 c に提供するようにしたから、救助活動や復旧活動を適切かつ早急に行うために必要な個人情報をより好適に提供することができ、しかも、個人情報が漏洩する可能性をより低減することができる。

【0063】また、個人情報を送信しようとする先が情報登録サーバ 2 であるか否かを認証するための認証サーバ 3 を前記ネットワークに接続し、入力端末 1 a ~ 1 c では、認証サーバ 3 を利用し、個人情報を送信しようとする先が情報登録サーバ 2 であると認証したときに、個人情報を送信するようにしたから、入力端末 1 a ~ 1 c から情報登録サーバ 2 に個人情報を確実に送信することができ、個人情報が漏洩する可能性をさらに低減することができる。

【0064】さらに、災害発生の際に、情報登録サーバ 2 に登録されている個人情報を利用しようとするときに、入力端末 1 a ~ 1 c と情報登録サーバ 2 とで、個人情報を利用しようとする者が特定者であるか否かを認証するようにしたら、特定者以外の者に個人情報が誤って提供される可能性を低減することができ、個人情報が漏洩する可能性をさらに低減することができる。

【0065】次に、本発明の第 2 の実施の形態を説明する。この第 2 の実施の形態は、本発明に係る災害時情報システムを、図 1 に示すように、各地に設置された入力端末と、情報登録サーバと、認証サーバと、をネットワークに接続し、災害発生の際に、各入力端末で個人情報として個人の安否に関する安否情報を入力する一方で、登録されている安否情報を家族等が利用するのに適用したものであって、上記第 1 の実施の形態と同一に構成されている。

【0066】認証サーバ 3 は、情報登録サーバ 2 に登録されている個人情報に係る者と特定の関係を有する家族等の関係者の公開鍵を登録するようになっている。入力端末 1 a ~ 1 c の演算処理装置 5 は、安否情報を入力しようとするときには、図 7 (a) のフローチャートに示す処理を実行し、災害発生の際に、情報登録サーバ 2 に登録されている安否情報を利用しようとするときには、図 7 (b) のフローチャートに示す処理を実行するようになっている。

【0067】つまり、入力端末 1 a ~ 1 c の演算処理装置 5 で、安否情報を入力しようとするときに実行される処理は、次のように構成されている。まず、図 7 (a) に示すように、ステップ S 4 1 に移行して、安否情報をキーボード 8 より入力し、ステップ S 4 2 に移行して、情報登録サーバ 2 より認証情報を取得し、ステップ S 4 3 に移行するようになっている。

【0068】ステップ S 4 3 では、認証サーバ 3 より情報登録サーバ 2 の公開鍵を取得し、ステップ S 4 4 に移行して、取得した情報登録サーバ 2 の公開鍵で認証情報を復号化し、ステップ S 4 5 に移行して、認証情報が正

常に復号化されたか否かを判定し、正常に復号化されたと判定されたときには、ステップS46に移行して、そうでないと判定されたときには、ステップS42に移行するようになっている。

【0069】ステップS46では、安否情報を情報登録サーバ2に送信し、一連の処理を終了するようになっている。また、入力端末1a～1cの演算処理装置5で、災害発生の際に、情報登録サーバ2に登録されている安否情報を利用しようとするときに実行される処理は、次のように構成されている。まず、図7(b)に示すように、ステップS51に移行して、要求する安否情報に係る者の名前をキーボード8より入力し、ステップS52に移行して、安否情報を要求する者の秘密鍵をキーボード8より入力し、ステップS53に移行して、安否情報を要求する者の秘密鍵で認証情報を暗号化し、ステップS54に移行するようになっている。

【0070】ステップS54では、暗号化した認証情報を情報登録サーバ2に送信し、ステップS55に移行して、情報登録サーバ2より安否情報を受信したか否かを判定し、受信したと判定されたときには、ステップS56に移行して、安否情報を要求する者の秘密鍵で受信した安否情報を復号化し、ステップS57に移行して、復号化した安否情報をCRT11に表示し、一連の処理を終了するようになっている。

【0071】一方、ステップS55で、情報登録サーバ2より安否情報を受信しないと判定されたときには、ステップS58に移行して、所定のエラー処理を実行し、一連の処理を終了するようになっている。

【0072】また一方、情報登録サーバ2の演算処理装置5は、入力端末1a～1cより安否情報の登録が要求されたときには、図8(a)のフローチャートに示す処理を実行し、災害発生の際に、入力端末1a～1cより安否情報の提供が要求されたときには、図8(b)のフローチャートに示す処理を実行するようになっている。

【0073】つまり、情報登録サーバ2の演算処理装置5で、入力端末1a～1cより安否情報の登録が要求されたときに実行される処理は、次のように構成されている。まず、図8(a)に示すように、ステップS61に移行して、情報登録サーバ2の秘密鍵で認証情報を暗号化し、ステップS62に移行して、暗号化した認証情報を登録要求のあった入力端末1a～1cに送信し、ステップS63に移行するようになっている。

【0074】ステップS63では、登録要求のあった入力端末1a～1cより安否情報を受信したか否かを判定し、受信したと判定されたときには、ステップS64に移行して、受信した安否情報を補助記憶装置7の所定領域に登録し、一連の処理を終了するようになっている。

【0075】一方、ステップS63で、登録要求のあった入力端末1a～1cより安否情報を受信しないと判定されたときには、ステップS65に移行して、所定のエ

ラー処理を実行し、一連の処理を終了するようになっている。

【0076】また、情報登録サーバ2の演算処理装置5で、災害発生の際に、入力端末1a～1cより安否情報の提供が要求されたときに実行される処理は、次のように構成されている。まず、図8(b)に示すように、ステップS71に移行して、入力端末1a～1cより送信される認証情報を受信し、ステップS72に移行して、要求のあった者の公開鍵を認証サーバ3より取得し、ステップS73に移行するようになっている。

【0077】ステップS73では、要求のあった者の公開鍵で認証情報を復号化し、ステップS74に移行して、認証情報が正常に復号化されたか否かを判定し、正常に復号化されたと判定されたときには、ステップS75に移行して、該当する安否情報を要求のあった者の公開鍵で暗号化し、ステップS76に移行して、暗号化した安否情報を要求のあった入力端末1a～1cに送信し、一連の処理を終了するようになっている。

【0078】一方、ステップS74で、認証情報が正常に復号化されないと判定されたときには、ステップS77に移行して、所定のエラー処理を実行し、一連の処理を終了するようになっている。

【0079】次に、上記第2の実施の形態の動作を図面を参照しながら説明する。始めに、災害が発生した際に、本人、医師または公営機関などがいずれかの入力端末1a～1cを利用し、安否情報を情報登録サーバ2に登録する場合について説明する。

【0080】まず、本人、医師または公営機関などが安否情報を情報登録サーバ2に登録しようとするには、各地に設置されているいずれかの入力端末1a～1c、例えば入力端末1aを利用し、安否情報を入力する。

【0081】そうすると、入力端末1aでは、安否情報を送信しようとする先が情報登録サーバ2であるか否かが認証され、送信しようとする先が情報登録サーバ2であると認証されたときに、入力された安否情報が情報登録サーバ2に送信される。

【0082】情報登録サーバ2では、入力端末1aより安否情報が送信されると、補助記憶装置7にその安否情報が登録される。なお、入力端末1aでは、安否情報を送信しようとする先が情報登録サーバ2でないと認証されたときには、情報登録サーバ2であると認証されるまで、ネットワークに接続されたコンピュータに対して認証を実行し続ける。また、情報登録サーバ2では、入力端末1aより安否情報の登録要求があったにもかかわらず、入力端末1aより個人情報が送信されないときには、エラー処理が実行される。

【0083】その次に、災害が発生した際に、個人情報に係る者と特定の関係を有する家族等の関係者が情報登録サーバ2に登録されている安否情報を利用しようとする場合について説明する。

【0084】まず、家族等が情報登録サーバ2に登録されている安否情報を利用するには、各地に設置されているいずれかの入力端末1a～1c、例えば入力端末1cを利用し、利用しようとする安否情報に係る者の名前を入力するとともに、安否情報を利用しようとする家族等の秘密鍵を入力する。

【0085】そうすると、入力端末1cでは、情報登録サーバ2に安否情報の提供が要求されるとともに、入力された秘密鍵に基づいて、情報登録サーバ2に対して安否情報を利用しようとする者が利用適格を有する者（認証サーバ3に公開鍵を登録した家族等）であることが証明される。

【0086】情報登録サーバ2では、安否情報を利用しようとする者が利用適格を有する者であると認証されると、該当する個人情報とその利用適格を有する者の公開鍵で暗号化され入力端末1cに送信される。

【0087】入力端末1cでは、情報登録サーバ2より安否情報が送信されると、安否情報を利用しようとする家族等の秘密鍵でその安否情報が復号化され、CRT制御装置10によりCRT11に表示される。

【0088】なお、情報登録サーバ2では、安否情報を利用しようとする者が利用適格を有しない者であると認証されたときには、その旨が入力端末1cに送信される。入力端末1cでは、これを受信すると、エラー処理が実行される。

【0089】このようにして、情報登録サーバ2に登録する個人情報には、個人の安否に関する安否情報を含ませるようにしたから、災害発生の際に、安否情報をその家族等に好適に提供することができる。

【0090】また、入力端末1a～1cは、情報登録サーバ2から安否情報を取得する際に、家族等の秘密鍵で暗号化した認証情報を情報登録サーバ2に送信し、情報登録サーバ2から安否情報を取得したときに、安否情報を家族等の秘密鍵で復号化し、情報登録サーバ2は、入力端末1a～1cから認証情報が送信された場合に、認証サーバ3から家族等の公開鍵を取得し、取得した公開鍵で認証情報を復号化し、正常に復号化されたときに、安否情報を家族等の公開鍵で暗号化して入力端末1a～1cに提供するようにしたから、個人情報が漏洩する可能性を低減することができる。

【0091】なお、上記第1および第2の実施の形態においては、個人情報および安否情報を送信しようとする先が情報登録サーバ2であることを認証してから、個人情報および安否情報を送信するように構成したが、これに限らず、情報登録サーバ2の認証を行わずに、個人情報および安否情報を送信するように構成してもよい。

【0092】また、上記第2の実施の形態においては、安否情報を関係者の公開鍵で暗号化して入力端末1a～1cに提供するように構成したが、これに限らず、安否情報を特に暗号化しないで入力端末1a～1cに提供す

るように構成してもよい。

【0093】さらに、上記第1および第2の実施の形態においては、個人情報を登録しおよび利用する構成と、安否情報を登録しおよび利用する構成とを別に構成したが、これに限らず、個人情報および安否情報をともに登録しおよび利用するように構成にしてもよい。

【0094】さらに、上記第1および第2の実施の形態においては、入力端末1a～1c、情報登録サーバ2および認証サーバ3のみをネットワークに接続するように構成したが、これに限らず、例えば、家族等の金銭の額を管理する請求項6記載の金額管理装置としての金額管理装置をネットワークに接続し、入力端末1a～1cは、災害発生の際に、特定者の要求に応じて金額管理装置で管理されている特定者の金銭の額を義援金として提供するように構成してもよい。このような構成であれば、簡単な手続きで義援金を提供することができる。

【0095】さらに、上記第1および第2の実施の形態において、入力端末1a～1cおよび情報登録サーバ2の演算処理装置5で図5～図8のフローチャートに示す処理を実行するにあたってはいずれも、主記憶装置6のROMにあらかじめ格納されているプログラムを実行する場合について説明したが、これに限らず、これらの手順を示したプログラムが記憶された記憶媒体から、そのプログラムを主記憶装置6のRAMに読み込んで実行するようにしてもよい。

【0096】ここで、記憶媒体とは、RAM、ROM、FD、コンパクトディスク、ハードディスク、光磁気ディスクまたは紙等の記憶媒体であって、電子的、磁氣的、光学的等の読み取り方法のいかににかかわらず、コンピュータで読み取り可能な記憶媒体であれば、あらゆる記憶媒体を含むものである。

【0097】さらに、上記第1および第2の実施の形態において、入力端末1a～1cおよび情報登録サーバ2の演算処理装置5で図5～図8のフローチャートに示す処理はいずれも、ソフトウェアで構成した場合について説明したが、これに代えて、比較回路、演算回路、論理回路等の電子回路を組み合わせるように構成してもよい。

【0098】上記実施の形態において、情報登録サーバ2は、請求項1、2または5記載の個人情報登録装置に対応し、認証サーバ3は、請求項3記載の第1の認証装置または請求項4記載の第2の認証装置に対応している。

【0099】また、ステップS2およびS3は、請求項2記載の暗号化処理に対応し、ステップS8は、請求項2記載の送信処理に対応し、ステップS11からS15までは、請求項2記載の取得処理に対応し、ステップS16は、請求項2記載の復号化処理に対応し、ステップS24は、請求項2記載の登録処理に対応し、ステップS31からS35までは、請求項2記載の提供処理に対

応している。

【0100】

【発明の効果】以上説明したように、本発明に係る災害時情報システムによれば、救助活動や復旧活動を適切かつ早急に行うために必要な個人情報を好適に提供することができ、しかも、個人情報が漏洩する可能性を低減することができるという効果が得られる。

【0101】また、本発明に係る請求項2記載の災害時情報システムによれば、個人情報が漏洩する可能性をより低減することができるという効果も得られる。さらに、本発明に係る請求項3記載の災害時情報システムによれば、入力端末から個人情報登録装置に個人情報を確実に送信することができるから、個人情報が漏洩する可能性をさらに低減することができるという効果も得られる。

【0102】さらに、本発明に係る請求項4記載の災害時情報システムによれば、災害発生の際に、個人の安否に関する情報をその家族等に好適に提供することができるという効果も得られる。

【0103】さらに、本発明に係る請求項5記載の災害時情報システムによれば、個人情報が漏洩する可能性をさらに低減することができるという効果も得られる。さらに、本発明に係る請求項6記載の災害時情報システムによれば、簡単な手続きで義援金を提供することができるという効果も得られる。

【図面の簡単な説明】

【図1】第1の実施の形態の構成を示すブロック図であ

る。

【図2】入力端末1a～1c、情報登録サーバ2および認証サーバ3の構成を示すブロック図である。

【図3】認証サーバ3における特定者の公開鍵の登録方式を示す図である。

【図4】情報登録サーバ2における個人情報の登録方式を示す図である。

【図5】入力端末1a～1cの演算処理装置5で実行される処理を示すフローチャートである。

【図6】情報登録サーバ2の演算処理装置5で実行される処理を示すフローチャートである。

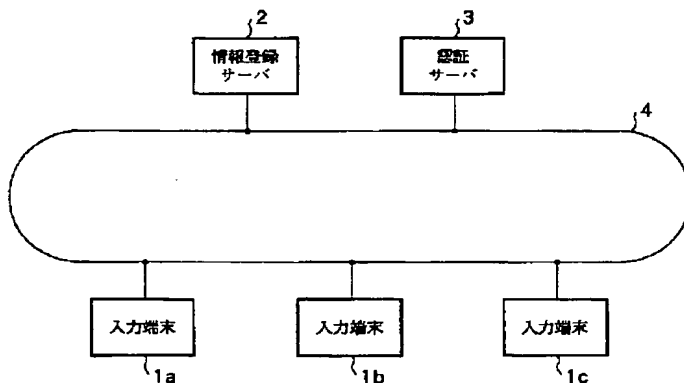
【図7】入力端末1a～1cの演算処理装置5で実行される処理を示すフローチャートである。

【図8】情報登録サーバ2の演算処理装置5で実行される処理を示すフローチャートである。

【符号の説明】

1 a ～ 1 c	入力端末
2	情報登録サーバ
3	認証サーバ
4	データ伝送路
5	演算処理装置
6	主記憶装置
7	補助記憶装置
8	キーボード
9	インターフェース部
1 0	C R T 制御装置
1 1	C R T

【図1】



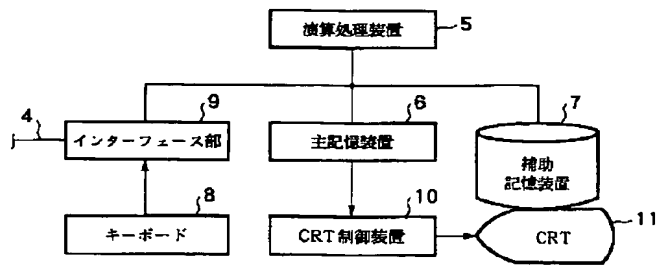
【図3】

名前	身体情報	連絡先情報	建物構造情報
A	M ₁	A ₁	S ₁
B	M ₂	A ₂	S ₂
C	M ₃	A ₃	S ₃
...
Z	M _n	A _n	S _n

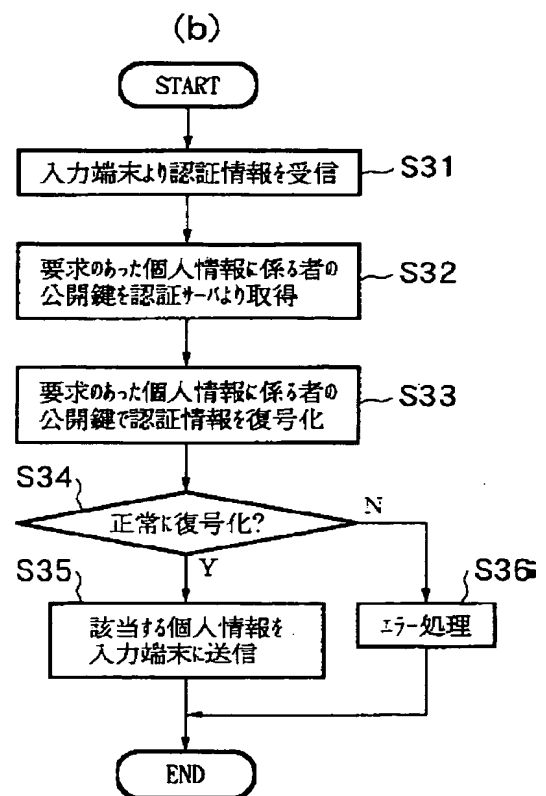
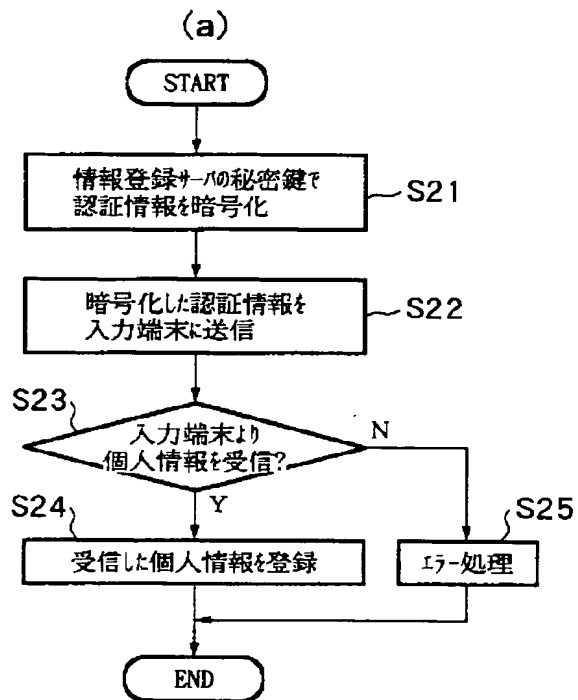
【図4】

名前	公開鍵
A	KO ₁
B	KO ₂
C	KO ₃
...	...
Z	KO _n

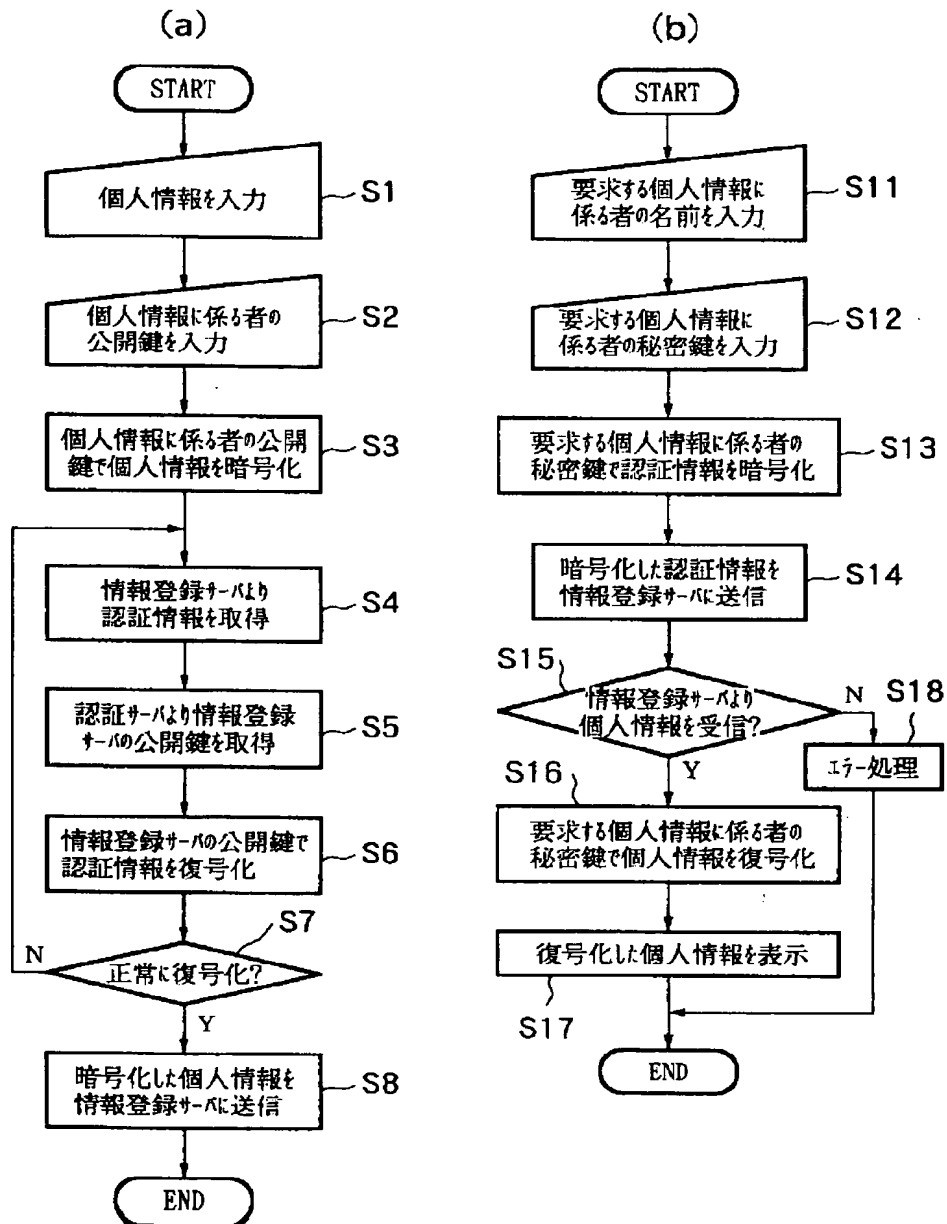
【図 2】



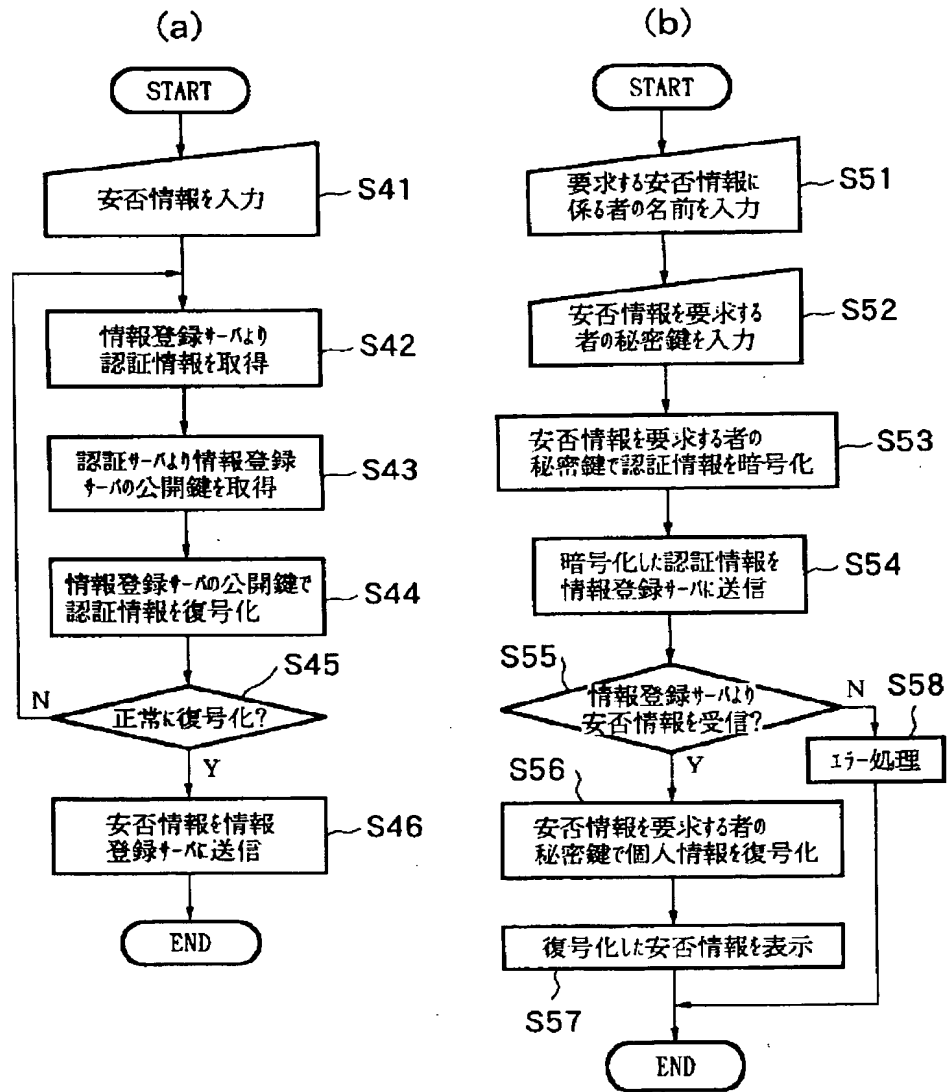
【図 6】



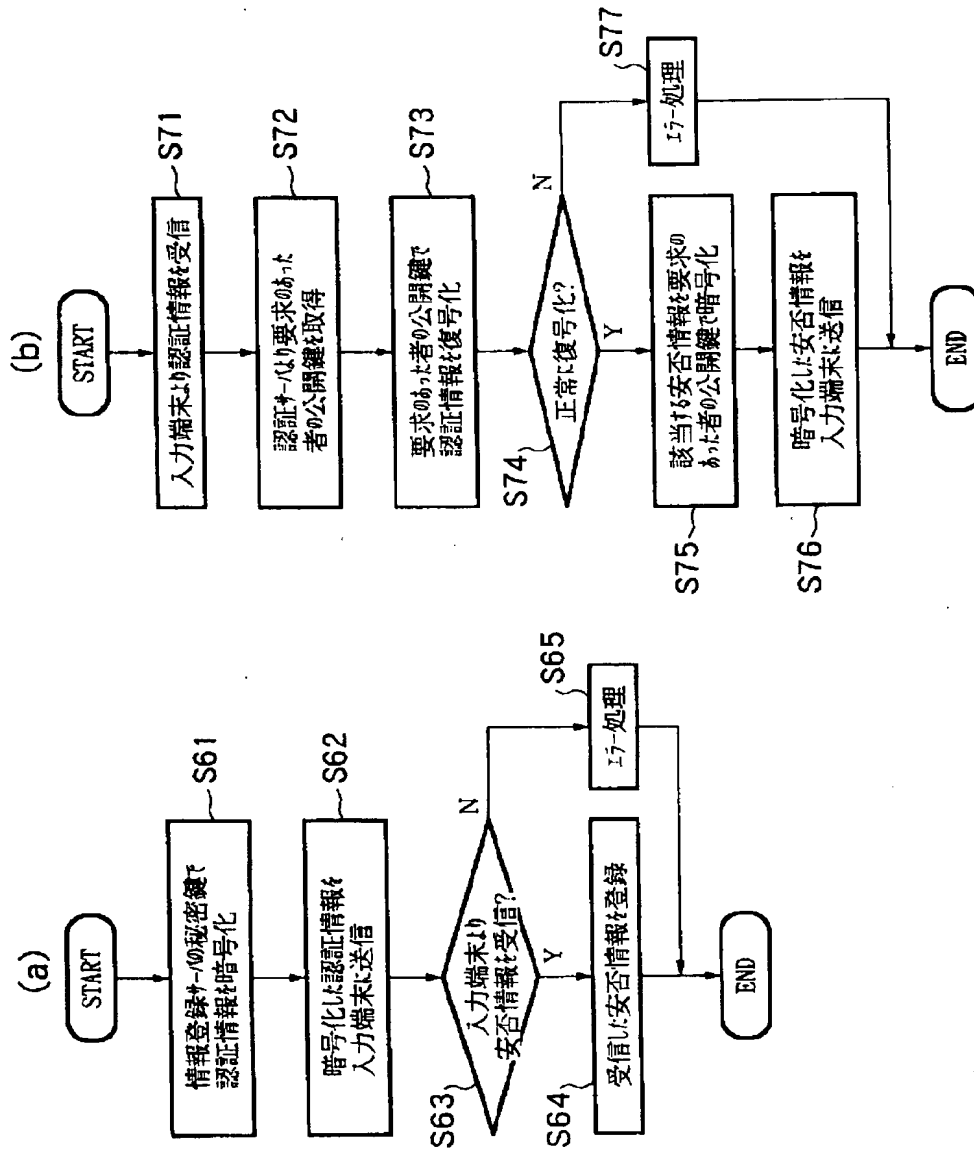
【図 5】



【図7】



【図 8】



フロントページの続き

(51)Int.Cl.⁶

H 0 4 M 11/04

識別記号

F I

H 0 4 L 11/02

Z